UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/084,436	02/28/2002	Zhichen Xu	10018744-1	6233

7590 12/17/2007

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
LEMMA, SAMSON B	
ART UNIT	PAPER NUMBER
2132	
MAIL DATE	DELIVERY MODE
12/17/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte ZHICHEN XU and LI XIAO

Appeal 2007-3452
Application 10/084,436
Technology Center 2100

Decided: December 17, 2007

Before HOWARD B. BLANKENSHIP, ST. JOHN COURTENAY III, and STEPHEN C. SIU, *Administrative Patent Judges*.

SIU, *Administrative Patent Judge*.

DECISION ON APPEAL

I. STATEMENT OF THE CASE

Appellants appeal under 35 U.S.C. § 134(a) from the Examiner's Final Rejection of claims 1-36. We have jurisdiction under 35 U.S.C. § 6(b). We reverse.

A. Invention

1The invention at issue involves providing privacy in a network system (Spec. 1). In particular, a user requests data from a data source and information responsive to the request is sent from the data source to the user over a network path of multiple peer nodes. A mix including the identity of each of the peer nodes in the network path is also generated for increasing privacy of the user (*Id.* 2-3).

B. Illustrative Claim

Claim 1, which further illustrates the invention, follows.

1. A method of increasing peer privacy in a computer network including peers operable to exchange information via the network, wherein the peers include computing platforms, the method comprising:

receiving a request for data from a data requestor;

determining whether a data provider exists that stores the requested data; wherein the data provider is a peer of the peers;

selecting a plurality of the peers to form a path between said data provider and said data requestor, wherein said data provider and said data requestor are the respective ends of said path;

generating a mix according to said path, wherein the mix includes an anonymous identity of each of the plurality of peers in the path; and

transmitting said mix to said data provider.

C. Rejection

Claims 1-36 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 5,862,223 ("Walker") and U.S. Patent No. 6,460,036 ("Herz").

II. ISSUES

Appellants assert that the combination of Walker and Herz fails to disclose selecting a plurality of peers to form a path between a data provider and a data requestor and generating a mix according to the path, as recited in claims 1, 18, and 24, or the mix including an anonymous identity of each of the plurality of peers in the path, and transmitting the mix to the data provider, as recited in claims 1, 14, 18, 22, and 24 (App. Br. 15-19).

In response, the Examiner asserts that Walker discloses using an "**anonymous mix 180 as part of a protocol to maintain anonymity between two people using a trusted third party**" (Ans. 15), that "there has to be some intermediate routers/peers that the path should follow before it finally reaches its destination" (*Id.*), and that "the expert answer could come from two different experts for one and the same request." (*Id.* 15-16). The Examiner further cites Herz at col. 37, ll. 45-52; col. 39, ll. 3-23; and col. 39, l. 66 – col. 40, l. 6 and argues that Herz discloses "pre-selecting the peers to be used in the mix, because the message is transmitted/returned along the pseudonymous **mix path specified by this return envelope set.**" (*Id.* 18).

Upon review of the record, Herz discloses a pseudonym containing "a unique string of bits . . . that is associated with a particular user" (col. 36, ll. 45-50) and "allows a service provider to communicate with users . . . while at the same time remaining ignorant of the users' true identities." (Col. 31, l. 65 – col. 32, l. 1). The user envelopes a message or request and sends the enveloped message to a proxy server (col. 37, ll. 47-52 and col. 39, ll. 3-23). The proxy server receives the enveloped message and creates a return

message along a pseudonymous mix path to the user (col. 39, l. 66 – col. 40, l. 6).

The cited portions of Herz disclose enveloping a message in a pseudonym and transmitting the enveloped message from a user to a proxy server where the proxy server creates and returns a message to the user along a pseudonymous mix path. Walker discloses an anonymous mix. We do not find that the combination of Herz and Walker encompasses the features recited in claims 1, 14, 18, 22, and 24. In particular, the combination of Walker and Herz, while disclosing sending an enveloped message from a user to a server, does not fairly teach or suggest a plurality of peers in the path and generating a mix that includes an identity of each of the peers in the plurality of peers in the path. The pseudonym of Herz is disclosed as corresponding to the user rather than any peers in the path. Thus, we find the combination of Herz and Walker fails to teach this feature.

Therefore, we reverse the rejection of claims 1, 14, 18, 22, and 24, and claims 2-13, 15-17, 19-21, 23, and 25-36, which depend therefrom.

III. ORDER

In summary, the rejection of claims 1-36 under § 103(a) is reversed.

REVERSED

clj

HEWLETT-PACKARD COMPANY
INTELLECTUAL PROPERTY ADMINISTRATION

P.O. BOX 272400
FORT COLLINS, CO 80527-2400